The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Bible Portal Project -- Bible Portal Project	PHP remote file inclusion vulnerability in Admin/rtf_parser.php in The Bible Portal Project 2.12 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the destination parameter.	unknown 2006-06-22	7.0	CVE-2006-3177 OTHER-REF FRSIRT SECUNIA
Chipmailer -- Chipmailer	Multiple SQL injection vulnerabilities in main.php in Chipmailer 1.09 allow remote attackers to execute arbitrary SQL commands via multiple parameters, as demonstrated by (1) anfang, (2) name, (3) mail, (4) anrede, (5) vorname, (6) nachname, (7) gebtag, (8) gebmonat, and (9) gebjahr.	unknown 2006-06-20	7.0	CVE-2006-3111 BUGTRAQ FRSIRT SECTRACK SECUNIA
CMS Faethon -- CMS Faethon	PHP remote file inclusion vulnerability in data/header.php in CMS Faethon 1.3.2 allows remote attackers to execute arbitrary PHP code via a URL in the mainpath parameter.	unknown 2006-06-22	7.0	CVE-2006-3185 BUGTRAQ BID FRSIRT SECUNIA
ComScripts -- CS-Forum	CRLF injection vulnerability in CS-Forum before 0.82 allows remote attackers to inject arbitrary email headers via a newline character in the email parameter to ajouter.php.	unknown 2006-06-22	7.0	CVE-2006-3171 OTHER-REF OTHER-REF FRSIRT SECUNIA
Content*Builder -- Content*Builder	Multiple PHP remote file inclusion vulnerabilities in Content*Builder 0.7.5 allow remote attackers to execute arbitrary PHP code via a URL with a trailing slash (/) character in the (1) lang_path parameter to (a) cms/plugins/col_man/column.inc.php, (b) cms/plugins/poll/poll.inc.php, (c) cms/plugins/user_managment/usrPortrait.inc.php, (d) cms/plugins/user_managment/user.inc.php, (e) cms/plugins/media_manager/media.inc.php, (f) cms/plugins/events/permanent.eventMonth.inc.php, (g) cms/plugins/events/events.inc.php, and (h) cms/plugins/newsletter2/newsletter.inc.php; (2) path[cb] paramter to (i) modules/guestbook/guestbook.inc.php, (j) modules/shoutbox/shoutBox.php, and (k) modules/sitemap/sitemap.inc.php; and the (3) rel parameter to (l) modules/download/overview.inc.php, (m) modules/download/detailView.inc.php, (n) modules/article/fullarticle.inc.php, (o) modules/article/comments.inc.php, (p) modules/article2/overview.inc.php, (q) modules/article2/fullarticle.inc.php, (r!) modules/article2/comments.inc.php, (s) modules/headline/headlineBox.php, and (t) modules/headline/showHeadline.inc.php.	unknown 2006-06-22	7.0	CVE-2006-3172 BUGTRAQ BID FRSIRT OSVDB SECUNIA
Content*Builder -- Content*Builder	Multiple PHP remote file inclusion vulnerabilities in Content*Builder 0.7.5 allow remote attackers to execute arbitrary PHP code via a URL in the (1) path[cb] parameter to (a) libraries/comment/postComment.php and (b) modules/poll/poll.php, (2) rel parameter to (c) modules/archive/overview.inc.php, and the (3) actualModuleDir parameter to	unknown 2006-06-22	7.0	CVE-2006-3173 SECUNIA

	(d) modules/forum/showThread.inc.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.			
Edge -- eCommerce Shop	Cross-site scripting (XSS) vulnerability in productDetail.asp in Edge eCommerce Shop allows remote attackers to inject arbitrary web script or HTML via the cart_id parameter.	unknown 2006-06-22	7.0	CVE-2006-3137 FRSIRT BLOGSPOT
Hosting Controller -- Hosting Controller	Unspecified vulnerability in Hosting Controller before 6.1 (aka Hotfix 3.2) allows remote authenticated attackers to gain host admin privileges, list all resellers, or change resellers' passwords via unspecified vectors. NOTE: due to the lack of precise details, it is not clear whether this is related to a previously disclosed issue such as CVE-2005-1788.	unknown 2006-06-22	7.0	CVE-2006-3147 OTHER-REF FRSIRT SECUNIA
hotwebscripts -- CMS Mundo	SQL injection vulnerability in controlpanel/index.php in CMS Mundo before 1.0 build 008 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2006-05-30 2006-06-21	7.0	CVE-2006-2911 BID FRSIRT OTHER-REF SECTRACK SECUNIA
IBD -- Micro CMS	PHP remote file inclusion vulnerability in microcms-include.php in IBD Micro CMS 0.3.5 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the microcms_path parameter.	unknown 2006-06-22	7.0	CVE-2006-3144 FRSIRT OTHER-REF SECUNIA
IMGallery -- IMGallery	Multiple SQL injection vulnerabilities in galeria.php in IMGallery 2.4 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) start or (2) sort parameters.	unknown 2006-06-22	7.0	CVE-2006-3163 BID FRSIRT OTHER-REF SECUNIA
iPostMX -- iPostMX 2005	Multiple SQL injection vulnerabilities in iPostMX 2005 2.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) forum parameter in messagepost.cfm and (2) topic parameter in topics.cfm. NOTE: this item was created based on information in a blog entry that was apparently removed after CVE analysis. As of 20060619, CVE is attempting to determing the cause of the removal.	unknown 2006-06-19	7.0	CVE-2006-3096 BLOGSPOT
mcGuestbook -- mcGuestbook	Multiple PHP remote file inclusion vulnerabilities in mcGuestbook 1.3 allow remote attackers to execute arbitrary PHP code via a URL in the lang parameter to (1) admin.php, (2) ecrire.php, and (3) lire.php.	unknown 2006-06-22	7.0	CVE-2006-3175 BUGTRAQ BID
Microsoft -- Hyperlink Object Library	Buffer overflow in Microsoft Hyperlink Object Library (hlink.dll) allows remote attack vectors to cause a denial of service (crash) and possibly execute arbitrary code via a long hyperlink, as demonstrated using an Excel worksheet with a long link in Unicode. NOTE: this is a different issue than CVE-2006-3059.	unknown 2006-06-19	7.0	CVE-2006-3086 OTHER-REF BID FULLDISC OTHER-REF FRSIRT SECUNIA
MobeScripts -- Mobile Space Community	SQL injection vulnerability in index.php in Mobile Space Community 2.0 allows remote attackers to execute arbitrary SQL commands via the browse parameter.	unknown 2006-06-22	7.0	CVE-2006-3181 BUGTRAQ FRSIRT OSVDB SECUNIA
MobeScripts -- Mobile Space Community	Directory traversal vulnerability in index.php in Mobile Space Community 2.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the uid parameter in the rss page.	unknown 2006-06-22	7.0	CVE-2006-3182 BUGTRAQ FRSIRT OSVDB SECUNIA
MobeScripts -- Mobile Space Community	Cross-site scripting (XSS) vulnerability in index.php in Mobile Space Community 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) browse parameter, which is not filtered in the resulting error message, and multiple unspecified input fields, including those involved when (2) updating a profile, (3) posting comments or entries in a blog, (4) uploading files, (5) picture captions, and (6) sending a private message (PM).	unknown 2006-06-22	7.0	CVE-2006-3183 BUGTRAQ FRSIRT OSVDB SECUNIA
Nucleus Group -- Nucleus CMS	Multiple PHP remote file inclusion vulnerabilities in Nucleus 3.23 allow remote attackers to execute arbitrary PHP code via a URL the DIR_LIBS parameter in (1) path/action.php, and to files in path/nucleus including (2) media.php, (3) /xmlrpc/server.php, and (4) /xmlrpc/api_metaweblog.inc.php. NOTE: this is a similar vulnerability to CVE-2006-2583.	unknown 2006-06-22	7.0	CVE-2006-3136 BID BUGTRAQ FRSIRT
openCI -- openCI	SQL injection vulnerability in index.php in openCI 1.0 BETA 0.20.1 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-06-22	7.0	CVE-2006-3140 OTHER-REF

Phorum -- Phorum	** DISPUTED ** PHP remote file inclusion vulnerability in common.php in PHORUM 5.1.13 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the PHORUM[http_path] parameter. NOTE: this issue has been disputed by the vendor, who states "common.php is checked on the very first line of non-comment code that it is not being called directly. It has been this way in all 5.x version of Phorum." CVE analysis concurs with the vendor.	unknown 2006-06-16	7.0	CVE-2006-3053 BUGTRAQ BID XF BUGTRAQ
phpMyDirectory -- phpMyDirectory	Multiple cross-site scripting (XSS) vulnerabilities in phpMyDirectory 10.4.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) PIC parameter in offers-pix.php, (2) from parameter in cp/index.php, and (3) action parameter in cp/admin_index.php.	unknown 2006-06-22	7.0	CVE-2006-3138 FRSIRT BLOGSPOT
saPHP -- saPHPLesson	SQL injection vulnerability in misc.php in SaphpLesson 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the action parameter.	unknown 2006-06-22	7.0	CVE-2006-3161 BID BUGTRAQ SECTRACK
SmartSiteCMS -- SmartSiteCMS	PHP remote file inclusion vulnerability in include/inc_foot.php in SmartSiteCMS 1.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the root parameter.	unknown 2006-06-22	7.0	CVE-2006-3162 FRSIRT OTHER-REF SECUNIA
SWSoft -- Confixx	Cross-site scripting (XSS) vulnerability in tools_ftp_pwaendern.php in Confixx Pro 3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the account parameter.	unknown 2006-06-22	7.0	CVE-2006-3179 BUGTRAQ FRSIRT SECUNIA
SWSoft -- Confixx	Cross-site scripting (XSS) vulnerability in ftp_index.php in Confixx Pro 3.0 allows remote attackers to inject arbitrary web script or HTML via the path parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-22	7.0	CVE-2006-3180 FRSIRT SECUNIA
TPL Design -- tplShop	SQL injection vulnerability in category.php in TPL Design tplShop 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the first_row parameter.	unknown 2006-06-22	7.0	CVE-2006-3164 BID FRSIRT OTHER-REF SECUNIA
TWiki -- TWiki	TWiki 4.0.0, 4.0.1, and 4.0.2 allows remote attackers to gain Twiki administrator privileges via a TWiki.TWikiRegistration form with a modified action attribute that references the Sandbox web instead of the user web, which can then be used to associate the user's login name with the WikiName of a member of the TWikiAdminGroup.	unknown 2006-06-20	8.0	CVE-2006-2942 TWIKI BID FRSIRT SECTRACK SECUNIA
VBZooM -- VBZooM	SQL injection vulnerability in Forum.php in VBZooM 1.11 allows remote attackers to execute arbitrary SQL commands via the MainID parameter.	unknown 2006-06-22	7.0	CVE-2006-3142 BID BUGTRAQ
VWar -- Virtual War	Multiple SQL injection vulnerabilities in war.php in Virtual War 1.5.0 R14 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) s, (2) showgame, (3) sortorder, and (4) sortby parameters.	unknown 2006-06-22	7.0	CVE-2006-3139 FRSIRT OTHER-REF SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AssoCIateD -- AssoCIateD CMS	Cross-site scripting (XSS) vulnerability in index.php in AssoCIateD (aka ACID) 1.2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the menu parameter.	unknown 2006-06-22	4.7	CVE-2006-3151 FRSIRT OTHER-REF SECUNIA
Bitweaver -- Bitweaver	Cross-site scripting (XSS) vulnerability in Bitweaver 1.3 allows remote attackers to inject arbitrary web script or HTML via the (1) error parameter in users/login.php and the (2) feedback parameter in articles/index.php.	2006-06-17 2006-06-20	4.7	CVE-2006-3103 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Bitweaver -- Bitweaver	CRLF injection vulnerability in Bitweaver 1.3 allows remote attackers to conduct HTTP response splitting attacks by via CRLF sequences in multiple unspecified parameters that are injected into HTTP headers, as demonstrated by the BWSESSION parameter in index.php.	2006-06-17 2006-06-20	4.7	CVE-2006-3105 BUGTRAQ OTHER-REF
Bluehouse Project -- phpTRADER	Multiple SQL injection vulnerabilities in phpTRADER 4.9 SP5 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) sectio parameter in (a) login.php, (b) write_newad.php, (c) newad.php, (d) printad.php, (e) askseller.php, (f) browse.php, (g) showmemberads.php, (h) note_ad.php, (i)	unknown 2006-06-22	4.7	CVE-2006-3152 FRSIRT OTHER-REF SECUNIA

	abuse.php, (j) buynow.php, (k) confirm_newad.php, (2) an parameter in (l) printad.php, (m) note_ad.php, (3) who parameter in (n) showmemberads.php, and (4) adnr parameter in (o) buynow.php.			
CavoxCms -- CavoxCms	SQL injection vulnerability in index.php in CavoxCms 1.0.16 and earlier allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2006-06-22	4.7	CVE-2006-3150 BID FRSIRT OTHER-REF SECUNIA
Cisco -- Secure ACS for Unix	Cross-site scripting (XSS) vulnerability in LogonProxy.cgi in Cisco Secure ACS for UNIX 2.3 allows remote attackers to inject arbitrary web script or HTML via the (1) error, (2) SSL, and (3) Ok parameters.	2006-01-27 2006-06-20	4.7	CVE-2006-3101 BUGTRAQ BUGTRAQ CISCO BID SECTRACK SECUNIA FRSIRT
Clubpage -- Clubpage	SQL injection vulnerability in index.php in Clubpage allows remote attackers to execute arbitrary SQL commands via the category parameter.	2006-06-20 2006-06-21	4.7	CVE-2006-3130 FRSIRT OTHER-REF SECUNIA
Clubpage -- Clubpage	Multiple cross-site scripting (XSS) vulnerabilities in Clubpage allow remote attackers to inject arbitrary web script or HTML via the (1) news_archive, (2) language, and (3) intranetLogin parameters in (a) index.php; the (4) sites_id parameter in (b) sites.php; and the (5) news_id parameter in (c) news_more.php.	2006-06-20 2006-06-21	4.7	CVE-2006-3131 FRSIRT OTHER-REF SECUNIA
ComScripts -- CS-Forum	SQL injection vulnerability in CS-Forum before 0.82 allows remote attackers to execute arbitrary SQL commands via the (1) id and (2) debut parameters in (a) read.php, and the (3) search and (4) debut parameters in (b) index.php.	unknown 2006-06-22	4.7	CVE-2006-3168 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
ComScripts -- CS-Forum	Multiple cross-site scripting (XSS) vulnerabilities in CS-Forum 0.81 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) msg_result and (2) rep_titre parameters in (a) read.php; and the (3) id and (4) parent parameters and (5) CSForum_nom, (6) CSForum_mail, and (7) CSForum_url cookie parameters in (b) ajouter.php.	unknown 2006-06-22	4.7	CVE-2006-3169 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
Docebo -- Docebo	Multiple PHP remote file inclusion vulnerabilities in Docebo 3.0.3 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in (1) GLOBALS[where_framework] to (a) admin/modules/news/news_class.php and (b) admin/modules/content/content_class.php, and (2) GLOBALS[where_cms] to (c) admin/modules/block_media/util.media.php. NOTE: this issue might be resultant from a global overwrite vulnerability. This issue is similar to CVE-2006-2576, but the vectors are different.	2006-06-09 2006-06-20	4.7	CVE-2006-3107 SECTRACK
Eduha Meeting -- Eduha Meeting	index.php in Eduha Meeting does not properly restrict file extensions before permitting a file upload, which allows remote attackers to bypass security checks and upload or execute arbitrary php code via the add action.	unknown 2006-06-22	4.7	CVE-2006-3158 BID FRSIRT OTHER-REF SECUNIA
EmailArchitect -- Email Server	Cross-site scripting (XSS) vulnerability in EmailArchitect Email Server 6.1 allows remote attackers to inject arbitrary Javascript via an HTML div tag with a carriage return between the onmouseover attribute and its value, which bypasses the mail filter.	2006-06-07 2006-06-20	4.7	CVE-2006-3108 SECTRACK
Fredi Bach -- PhpMyDesktop|arcade	Cross-site scripting (XSS) vulnerability in index.php in phpMyDesktop|Arcade 1.0 allows remote attackers to inject arbitrary web script or HTML via the subsite parameter in the subsite todo.	2006-06-02 2006-06-20	4.7	CVE-2006-3106 SECTRACK
HotPlug CMS -- HotPlug CMS	Cross-site scripting (XSS) vulnerability in administration/tblcontent/login1.php in HotPlug CMS 1.0 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	unknown 2006-06-22	4.7	CVE-2006-3189 BUGTRAQ FRSIRT SECTRACK
hotwebscripts -- CMS Mundo	CMS Mundo before 1.0 build 008 does not properly verify uploaded image files, which allows remote attackers to execute arbitrary PHP code by uploading and later directly accessing certain files.	2006-05-30 2006-06-21	5.6	CVE-2006-2931 BID FRSIRT OTHER-REF SECTRACK SECUNIA

Microsoft -- Excel	Microsoft Excel allows user-complicit attackers to execute arbitrary code via an Excel spreadsheet with an embedded Shockwave Flash Object, which is automatically executed when the user opens the spreadsheet.	2006-05-03 2006-06-21	5.6	CVE-2006-3014 FULLDISC OTHER-REF
Microsoft -- Excel	Unspecified vulnerability in Microsoft Excel allows remote user-complicit attackers to execute arbitrary code via unspecified vectors. NOTE: as of 20060616, there is vague information about this vulnerability, although it is known that it is new. Also, as of 20060618, it is not clear whether this is the same issue as CVE-2006-3086.	unknown 2006-06-17	5.6	CVE-2006-3059 OTHER-REF CERT-VN BID FRSIRT SECTRACK SECUNIA CERT OTHER-REF OSVDB XF BUGTRAQ OTHER-REF
NC LinkList -- NC LinkList	Multiple cross-site scripting (XSS) vulnerabilities in index.php in NC LinkList 1.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) cat and (2) view parameters.	2006-06-19 2006-06-21	4.7	CVE-2006-3129 FRSIRT OTHER-REF
Open-Realty -- Open-Realty	SQL injection vulnerability, possibly in search.inc.php, in Open-Realty 2.3.1 allows remote attackers to execute arbitrary SQL commands via the sorttype parameter to index.php.	unknown 2006-06-22	4.7	CVE-2006-3148 FRSIRT OTHER-REF SECUNIA
PhpBlueDragon -- PhpBlueDragon CMS	PHP remote file inclusion vulnerability in software_upload/public_includes/pub_templates/vphptree/template.php in PhpBlueDragon CMS 2.9.1 allows remote attackers to execute arbitrary PHP code via a URL in the vsDragonRootPath parameter.	2006-06-14 2006-06-19	4.7	CVE-2006-3076 BUGTRAQ BID
phpMyForum -- phpMyForum	Cross-site scripting (XSS) vulnerability in topic.php in phpMyForum 4.1.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the highlight parameter.	unknown 2006-06-22	4.7	CVE-2006-3149 BID FRSIRT OTHER-REF SECUNIA
QTO -- QTOFileManager	Cross-site scripting (XSS) vulnerability in qtofm.php4 in QTOFileManager 1.0 allows remote attackers to inject arbitrary web script or HTML via the msg parameter, as originally reported to index.php.	2006-06-20 2006-06-21	4.7	CVE-2006-3132 BUGTRAQ FRSIRT SECTRACK SECUNIA
Thinkfactory -- Ultimate Estate	SQL injection vulnerability in index.pl in Ultimate Estate 1.0 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-06-22	4.7	CVE-2006-3154 FRSIRT OTHER-REF SECUNIA
Thinkfactory -- UltimateGoogle	Cross-site scripting (XSS) vulnerability in index.php in Thinkfactory UltimateGoogle 1.00 and earlier allows remote attackers to inject arbitrary web script or HTML via the REQ parameter.	unknown 2006-06-22	4.7	CVE-2006-3157 FRSIRT OTHER-REF SECUNIA
Ultimate eShop -- Ultimate eShop	Cross-site scripting (XSS) vulnerability in index.cgi in Ultimate eShop 1.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the subid parameter.	unknown 2006-06-22	4.7	CVE-2006-3156 OTHER-REF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
ASP Stats Generator -- ASP Stats Generator	Direct static code injection vulnerability in ASP Stats Generator before 2.1.2 allows remote authenticated attackers to execute arbitrary ASP code via the strAsgSknPageBgColour parameter to settings_skin.asp, which is stored in inc_skin_file.asp.	unknown 2006-06-22	2.3	CVE-2006-3184 OTHER-REF FRSIRT SECUNIA
Bitweaver -- Bitweaver	Race condition in articles/BitArticle.php in Bitweaver 1.3, when run on Apache with the mod_mime extension, allows remote attackers to execute arbitrary PHP code by uploading arbitrary files with double extensions, which are stored for a small period of time under the webroot in the temp/articles directory.	2006-06-17 2006-06-20	3.7	CVE-2006-3102 BUGTRAQ OTHER-REF FRSIRT SECUNIA
Bitweaver -- Bitweaver	users/index.php in Bitweaver 1.3 allows remote attackers to obtain sensitive information via an invalid sort_mode parameter, which reveals the installation path and database information in the resultant error message.	2006-06-17 2006-06-20	2.3	CVE-2006-3104 BUGTRAQ OTHER-REF FRSIRT SECUNIA

CFXe-CMS -- CFXe-CMS	Cross-site scripting (XSS) vulnerability in search.cfm in CreaFrameXe (CFXe) CMS 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the voltext_suche parameter.	unknown 2006-06-16	1.9	CVE-2006-3043 OTHER-REF FRSIRT SECUNIA SECTRACK
Chipmailer -- Chipmailer	Cross-site scripting (XSS) vulnerability in main.php in Chipmailer 1.09 allows remote attackers to inject arbitrary web script or HTML via the (1) name, (2) betreff, (3) mail, and (4) text parameters.	unknown 2006-06-20	2.3	CVE-2006-3110 BUGTRAQ SECTRACK
Chipmailer -- Chipmailer	Chipmailer 1.09 allows remote attackers to obtain sensitive information via a direct request to php.php, which displays the output of the phpinfo function.	unknown 2006-06-20	2.3	CVE-2006-3112 BUGTRAQ SECTRACK
Cisco -- Call Manager	Cross-site scripting (XSS) vulnerability in Cisco CallManager 3.3 before 3.3(5)SR3, 4.1 before 4.1(3)SR4, 4.2 before 4.2(3), and 4.3 before 4.3(1), allows remote attackers to inject arbitrary web script or HTML via the (1) pattern parameter in ccmadmin/phonelist.asp and (2) arbitrary parameters in ccmuser/logon.asp, aka bugid CSCsb68657.	2005-10-24 2006-06-20	2.3	CVE-2006-3109 FULLDISC BUGTRAQ OTHER-REF CISCO BID SECTRACK FRSIRT SECUNIA
CMS Faethon -- CMS Faethon	Multiple cross-site scripting (XSS) vulnerabilities in CMS Faethon 1.3.2 allow remote attackers to inject arbitrary web script or HTML via the mainpath parameter to (1) data/footer.php and (2) admin/header.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-22	2.3	CVE-2006-3186 FRSIRT SECUNIA
ComScripts -- CS-Forum	CS-Forum before 0.82 allows remote attackers to obtain sensitive information via unspecified manipulations, possibly involving an empty collapse[] or readall parameter to index.php, which reveals the installation path in an error message.	unknown 2006-06-22	2.3	CVE-2006-3170 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA
Dpivision -- Tradingeye Shop	Cross-site scripting (XSS) vulnerability in details.cfm in Tradingeye Shop R4 and earlier allows remote attackers to inject arbitrary web script or HTML via the image parameter.	unknown 2006-06-22	2.3	CVE-2006-3141 FRSIRT OTHER-REF SECUNIA
easy-CMS -- easy-CMS	choose_file.php in easy-CMS 0.1.2, when mod_mime is installed, does not restrict uploads of filenames with multiple extensions, which allows remote attackers to execute arbitrary PHP code by uploading a PHP file with a GIF file extension, then directly accessing that file in the Repositories directory.	unknown 2006-06-21	3.4	CVE-2006-3128 FRSIRT OTHER-REF SECTRACK SECUNIA
Free Realty -- Free Realty	SQL injection vulnerability in propview.php in Free Realty 2.9-0.7 and earlier allows remote attackers to execute arbitrary SQL commands via the sort parameter.	unknown 2006-06-22	2.3	CVE-2006-3165 BID FRSIRT OTHER-REF SECUNIA
Free Realty -- Free Realty	Cross-site scripting (XSS) vulnerability in propview.php in Free Realty 2.9-0.6 and earlier allows remote attackers to execute arbitrary web script or HTML via the sort parameter.	unknown 2006-06-22	2.3	CVE-2006-3166 OTHER-REF
Free Realty -- Free Realty	Free Realty before 2.9 allows remote attackers to obtain the full path and other sensitive information via unspecified manipulations that produce an error message.	unknown 2006-06-22	2.3	CVE-2006-3167 OTHER-REF
GnuPG -- GnuPG	parse-packet.c in GnuPG (gpg) 1.4.3 and 1.9.20, and earlier versions, allows remote attackers to cause a denial of service (gpg crash) and possibly overwrite memory via a message packet with a large length, which could lead to an integer overflow, as demonstrated using the --no-armor option.	unknown 2006-06-19	2.3	CVE-2006-3082 FULLDISC FULLDISC FULLDISC OTHER-REF
HotPlug CMS -- HotPlug CMS	SQL injection vulnerability in administration/includes/login/auth.php in HotPlug CMS 1.0 allows remote attackers to execute arbitrary SQL commands and bypass authentication via the (1) username and (2) password parameters.	unknown 2006-06-22	2.3	CVE-2006-3190 BUGTRAQ FRSIRT SECTRACK
HP -- HP-UX	Unspecified vulnerability in Support Tools Manager (xstm, cstm, and stm) on HP-UX B.11.11 and B.11.23 allows local users to cause an unspecified denial of service via unknown vectors.	unknown 2006-06-20	2.3	CVE-2006-3097 HP BID SECTRACK
Jed Wing -- CHM lib	Directory traversal vulnerability in extract_chmLib example program in CHM Lib (chmlib) before 0.38 allows remote attackers to overwrite arbitrary files via a CHM archive containing files with a .. (dot dot) in their filename.	unknown 2006-06-22	2.3	CVE-2006-3178 OTHER-REF FRSIRT SECUNIA

Maximus -- SchoolMAX	Cross-site scripting (XSS) vulnerability in icue_login.asp in Maximus SchoolMAX 4.0.1 and earlier iCue and iParent applications allows remote attackers to inject arbitrary web script or HTML via the error_msg parameter.	unknown 2006-06-22	3.7	CVE-2006-3143 BUGTRAQ FRSIRT SECUNIA
NetPBM -- NetPBM	Buffer overflow in pamtofits of NetPBM 10.30 through 10.33 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code when assembling the header, possibly related to an off-by-one error.	unknown 2006-06-22	2.3	CVE-2006-3145 BID OTHER-REF FRSIRT SECUNIA
Sharky e-shop -- Sharky e-shop	Multiple cross-site scripting (XSS) vulnerabilities in Sharky e-shop 3.05 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) maingroup and (2) secondgroup parameters to (a) search_prod_list.asp, and the (3) maingroup parameter to (b) meny2.asp. NOTE: it is possible that this is resultant from SQL injection or a forced SQL error.	unknown 2006-06-22	2.3	CVE-2006-3187 OTHER-REF FRSIRT
Sharky e-shop -- Sharky e-shop	Multiple SQL injection vulnerabilities in Sharky e-shop 3.05 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) maingroup and (2) secondgroup parameters to (a) search_prod_list.asp, and the (3) maingroup parameter to (b) meny2.asp. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-22	2.3	CVE-2006-3188 FRSIRT
Simple File Manager -- Simple File Manager	Cross-site scripting (XSS) vulnerability in fm.php in Simple File Manager (SFM) 0.24a and earlier allows remote attackers to inject arbitrary web script or HTML via the msg parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-22	1.9	CVE-2006-3160 BID FRSIRT SECUNIA
SquirrelMail -- SquirrelMail	Cross-site scripting (XSS) vulnerability in search.php in SquirrelMail 1.5.1 and earlier, when register_globals is enabled, allows remote attackers to inject arbitrary HTML via the mailbox parameter.	unknown 2006-06-22	2.3	CVE-2006-3174 OTHER-REF OSVDB
Sun -- Java Enterprise System	Memory leak in Network Security Services (NSS) 3.11, as used in Sun Java Enterprise System 2003Q4 through 2005Q1, allows remote attackers to cause a denial of service (memory consumption) by performing a large number of RSA cryptographic operations.	unknown 2006-06-21	3.3	CVE-2006-3127 SECTRACK SUNALERT
Sun -- ONE Messaging Server Sun -- iPlanet Messaging Server	pipe_master in Sun ONE/iPlanet Messaging Server 5.2 HotFix 1.16 (built May 14 2003) allows local users to read portions of restricted files via a symlink attack on msg.conf in a directory identified by the CONFIGROOT environment variable, which returns the first line of the file in an error message.	unknown 2006-06-22	1.6	CVE-2006-3159 FULLDISC SECTRACK
Think Factory -- Ultimate Estate	Multiple cross-site scripting (XSS) vulnerabilities in Ultimate Auction 1.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) item parameter in (a) emailtofriend.pl or (b) violation.pl, (2) seller parameter in (c) vsoa.pl, (3) user parameter in (d) userask.pl or (e) leavefeed.pl, (4) itemnum parameter in userask.pl, (5) category parameter in (f) itemlist.pl, and the (6) query parameter in (g) search.pl.	unknown 2006-06-22	2.3	CVE-2006-3155 OTHER-REF
Thinkfactory -- Ultimate Estate	Cross-site scripting (XSS) vulnerability in index.pl in Ultimate Estate 1.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the cat parameter.	unknown 2006-06-22	2.3	CVE-2006-3153 FRSIRT OTHER-REF SECUNIA
Toshiba -- Bluetooth Stack	The TOSRFBD.SYS driver for Toshiba Bluetooth Stack 4.00.23 and earlier on Windows allows remote attackers to cause a denial of service (reboot) via a L2CAP echo request that triggers an out-of-bounds memory access, similar to "Ping o' Death" and as demonstrated by BlueSmack.	unknown 2006-06-22	2.3	CVE-2006-3146 BID BUGTRAQ FRSIRT OTHER-REF SECUNIA
Xaran -- Xaran CMS	SQL injection vulnerability in xarancms_haupt.php in xarancms 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-06-22	2.3	CVE-2006-3176 OTHER-REF FRSIRT SECUNIA

Back to top

Last updated June 26, 2006